

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA**

UNITED STATES OF)	CASE NO. 8:17CR289
AMERICA,)	
)	
Plaintiff,)	BRIEF IN SUPPORT OF
)	MOTION TO SUPPRESS
)	EVIDENCE AND
v.)	STATEMENTS AND
)	REQUEST FOR
MARK RINGLAND,)	EVIDENTIARY HEARING
)	
Defendant.)	

Defendant Mark Ringland has moved to suppress all evidence seized in this case following the execution of numerous (at least 35) warrantless searches and seizures of his email by a government entity.

FACTS

Google, Inc. (“Google”) searched without warrant the contents of Mr. Ringland’s personal email addresses (“gmail” accounts) repeatedly between March 20, 2017 and September 1, 2017. These searches included files sent from Mr. Ringland to himself and files that were not sent at all. Google, having searched Mr. Ringland’s personal email addresses and finding what it believed to be contraband, forwarded the contents of those files to the National Center for Missing and Exploited Children (“NCMEC”), a government entity, in the form of CyberTips.

NCMEC, having received the files from Google, not only replicated but expanded upon the warrantless searches conducted by Google and made available to various law-enforcement agencies the contents of Mr. Ringland's personal emails. Before any warrant had been issued, an investigator with the Nebraska State Patrol had been

provided with and examined 502 files seized from Mr. Ringland's personal email accounts.

Supported by facts gleaned from these warrantless searches, on June 27, 2017 and August 7, 2017, Investigator C.J. Alberico of the Nebraska State Patrol sought and received two search warrants from Douglas County (NE) Court for the contents of Mr. Ringland's personal email (gmail) accounts, which were located in Google, Inc.'s servers in Mountain Valley, California. Throughout the process of obtaining these warrants, NCMEC and the Nebraska State Patrol continued to receive from Google (and review without warrant) the contents of Mr. Ringland's personal email accounts.

On August 31, 2017, Investigator Alberico applied for, and a United States magistrate judge signed, a search warrant/cell phone ping order. This warrant/order was issued to Sprint Spectrum LP for phone number 402-xxx-0902. The execution of that order provided law enforcement with Mr. Ringland's precise location.

On September 1, 2017, Investigator Alberico applied for, and a United States magistrate judge issued, a search warrant and a criminal complaint for Mark Ringland. That same day, Investigator Alberico, along with members of the Child Exploitation Task Force, FBI, NSP, and Douglas County Sheriff's Office, executed the warrant. Ringland's person was searched, pursuant to this warrant, by law enforcement. A ZTE cellular phone and an iPad were seized pursuant to the search warrant.

On September 1, 2017 and September 5, 2017, Mark Ringland made incriminatory statements to law-enforcement regarding his involvement in the offenses charged in the Indictment.

ANALYSIS

These warrantless searches and seizures by government agents and entities and their fruits – including the contents of Mark Ringland’s three gmail accounts, the contents of his two phone numbers, his location on August 31-September 1, 2017, the contents of his ZTE cell phone, the contents of his iPad, and his statements to law enforcement – violated of his Fourth Amendment rights under the United States Constitution.

This evidence must be suppressed.

A. Google acted an agent of the government.

Section 2258A of Title 18, U.S. Code, imposes a duty upon “whoever, while engaged in providing an electronic communication service or a remote computing service to the public through a facility or means of interstate or foreign commerce” to “provide to the CyberTipline of the National Center for Missing and Exploited Children” a report should the provider obtain actual knowledge of apparent violations of 18 U.S.C. §§ 1466A, 2251, 2251A, 2252, 2252A, 2252B, or 2260.

“[S]ince time out of mind the law has prevented agents from exercising powers their principals do not possess and cannot delegate.” *Ackerman*, 831 F.3d at 1300 (citing 1 William Blackstone, Commentaries *417-20 and Restatement (Second) of Agency § 17 (1958)). Here, the government (*i.e.*, NCMEC and the Nebraska State

Patrol) was heavily involved in and aware of the ongoing searches of Mr. Ringland's email accounts. Google, by reporting its findings to the government, aimed to help the government and to fulfill the legal duty imposed on internet service providers (ISP) by 18 U.S.C. § 2258A. "ISPs who fail to comply with this obligation face substantial (and apparently criminal) penalties payable to the federal government." *Ackerman*, 831 F.3d at 1296 (citing 18 U.S.C. § 2258A(a)(1)).

Nonetheless, the Eighth Circuit has held that "[a] reporting requirement standing alone, does not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography." *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013). But *Stevenson* was decided before *Riley v. California*, 134 S. Ct. 2473 (2014), where the Court held that law enforcement needs a warrant before they can search the content of an individual's cell phone. In *Riley*, the Court acknowledged how contemporary society views cell phones in the context of privacy concerns:

Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.

Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.

Id. at 2489.

The Court has espoused that there is a reasonable expectation of privacy in our digital lives and Google acting as Big Brother in light of the reporting requirement effectively turns them into a state actor for the purpose of needing a warrant to review a person's uploads to their servers.

In the present case, on 35 different occasions, Google, well aware of a pending investigation regarding Mr. Ringland (or at a minimum, concerning his gmail accounts) forwarded to NCMEC copies of files seized from unsent emails and emails sent between Mr. Ringland's accounts.

B. NCMEC is a government entity.

The Fourth Amendment applies only to state action. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). The “calling card of a governmental entity is whether it is ‘invested with any portion of political power, partaking in any degree in the administration of civil government, and performing duties which flow from sovereign authority.’” *United States v. Ackerman*, 831 F.3d 1292, 1295 (10th Cir. 2016) (*quoting Trustees of Dartmouth College v. Woodward*, 17 U.S. (4 Wheat.) 518, 668-69, 4 L.Ed. 629 (1819)).

The National Center for Missing and Exploited Children enjoys law-enforcement powers beyond those enjoyed by private citizens. Two statutes – 18 U.S.C. § 2258A and 34 U.S.C. § 11293(b) – “mandate its collaboration with federal (as well as state and local) law enforcement in over a dozen different ways, many of which involve duties and powers conferred on and enjoyed by NCMEC but no other private person.”

Ackerman, 831 F.3d at 1296. “NCMEC and NCMEC alone is statutorily obligated to maintain an electronic tipline for ISPs to report possible child sexual exploitation to the government.” *Id.* Moreover, ISPs are required to report contraband to NCMEC, who, in turn, requires the ISP to preserve the evidence. *See Ackerman*, 831 F.3d at 1297. Unlike private entities, NCMEC is allowed to receive contraband. *Id.*

Even if this Court adopts the reasoning of *Stevenson*, the Tenth Circuit’s opinion in *Ackerman* points out that, where NCMEC – a government entity – engages in a search that is more expansive than the one engaged in by the ISP, a Fourth Amendment search by a government entity – as opposed to a private entity – has occurred. *See* 831 F.3d at 1306.

C. A search occurred.

An email is a paper or effect for the purposes of the Fourth Amendment. *See, e.g., Ackerman*, 831 F3d at 1304 (“No one in this appeal [including the United States or amici curiae, NCMEC and Google, Inc.] disputes that an email is a ‘paper’ or ‘effect’ for Fourth Amendment purposes.”) Mr. Ringland had a reasonable expectation of privacy in his gmail accounts. The warrantless review of the contents of those accounts by Google and NCMEC infringed upon Mr. Ringland’s reasonable expectation of privacy.

That said, the “reasonable expectation of privacy” formulation is not the only way a Fourth Amendment search can occur. A search can occur “*either* when it infringes upon a reasonable expectation of privacy *or* when it involves a physical

intrusion (a trespass) on a constitutionally protected space or thing (“persons, houses, papers, and effects”) for the purpose of obtaining information.” *Ackerman*, 831 F.3d at 1307 (citing *United States v. Jones*, — U.S. —, 132 S.Ct. 945 (2012) (emphasis in original)). The warrantless opening and examination of private correspondence that could have contained much besides contraband “seems pretty clearly to qualify as exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment.” *Ackerman*, 831 at 1307-08 (citing, e.g., 1 Thomas M. Cooley, *The General Principles of Constitutional Law in the United States of America* 212 & n. 2 (1880); Thomas M. Cooley, *A Treatise on the Constitutional Limitations Which Rest Upon the Legislative Power of the States of the American Union* 306 n.2 (1868); and *Ex Parte Jackson*, 96 U.S. 727, 733 (1877)).

D. Warrantless searches of private correspondence by government agents and government entities are violations of the Fourth Amendment.

No cognizable exception to the Warrant Requirement exists here. Suppression of the evidence obtained illegally as a result of the warrantless searches by Google, NCMEC, and the Nebraska State Patrol is the proper remedy. As such, all evidence seized from Ringland’s gmail accounts, his person, his ZTE cell phone, and his iPad, as well as all statements taken from him, should be suppressed as fruit of the illegal search and the illegal search warrant execution. *Wong Sun v. United States*, 371 U.S. 471, 487-88 (1963).

CONCLUSION

WHEREFORE, Mark Ringland requests that this Court grant his motion to suppress all evidence obtained during and derived from (as a “fruit” of) these warrantless searches and seizures. Because of the highly factual nature of this motion, to include 35 CyberTips, four search-warrant applications, and four search warrants, Mr. Ringland requests an evidentiary hearing on this motion. Mr. Ringland puts the United States to its burden of proving compliance with the Fourth Amendment.

MARK RINGLAND, Defendant,

By: s/ Richard H. McWilliams
RICHARD H. MCWILLIAMS
Assistant Federal Public Defender
222 South 15th Street, Suite 300N
Omaha, NE 68102
(402) 221-7896
fax: (402) 221-7884
e-mail: rich_mcowilliams@fd.org

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document was filed with the Clerk of the District Court using the CM/ECF system which sent notification of such filing to Michael P. Norris, Assistant United States Attorney, on April 11, 2018.

By: s/ Richard H. McWilliams
RICHARD H. MCWILLIAMS